## REMARKS/ARGUMENTS

Claims 1-38 are pending in the present application. Claims 14, 16 and 30 have been amended herewith. Reconsideration of the claims is respectfully requested.

### I. Claim Objections

Claims 14, 16, 28 and 30 were objected to under 37 CFR 175 (c) as being of improper dependent form for failing to further limit the subject matter of a previous claim.

With respect to Claim 14, the Examiner notes that such claim does not further limit the method of Claim 1. Applicants have amended Claim 14 such that it further limits the 'identifying' step of Claim 1.

With respect to Claim 16, the Examiner notes that such claim does not recite any limitation that can be regarded as a structural element. Applicants have amended Claim 16 such that it further limits the 'selectively verifying means' of Claim 15.

With respect to Claim 28, the Examiner states that such claim does not recite any limitation that can be regarded as a structural element or structural interconnection further limiting the method of Claim 1. Applicants urge that Claim 28 depends upon system Claim 15, and therefore does not need to further limit Claim 1. In addition, Claim 28 recites a structural element (the particular structural location of the flags).

With respect to 30, the Examiner states that such claim does not recite any limitation that can be regarded as an instruction further limiting Claim 29. Applicants have amended Claim 30 such that it further limits the 'first instructions' of Claim 29.

Therefore, the objection to the claims has been overcome.

### II. 35 U.S.C. § 112, Second Paragraph

Claims 14, 16, 28 and 30 stand rejected under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential elements. This rejection is respectfully traversed.

The rejection of Claims 14, 16, 28 and 30 under 35 U.S.C. § 112, second paragraph essentially replicates the reasoning given in the objection to the claims. Thus, Applicants traverse the rejection of these claims under 35 U.S.C. § 112, second paragraph for reasons given above with respect to the claim objections.

Therefore, the rejection of Claims 14, 16, 28 and 30 under 35 U.S.C. § 112, second paragraph has been overcome.

## III. 35 U.S.C. § 101

Claims 29-38 stand rejected under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. This rejection is respectfully traversed.

The Examiner notes terminology in the present Specification at page 30 that can be interpreted to mean that recordable-type media includes transmission-type media. Applicants urge that such transmission-type media description was previously removed from the Specification (Response to Office Action filed on February 6, 2008), and thus the Examiner's quotation of "recordable-type media" being defined in the Specification as encompassing "transmission-type media" is erroneous, as the Specification defines recordable-type media to b media such as floppy disk, a hard disk drive, a RAM, CD-ROMs, and DVD-ROMs. Importantly, Claim 29 is directed to recordable-type media, and is not directed transmission-type media.

Therefore, the rejection of Claims 29-38 under 35 U.S.C. § 101 has been overcome.

## IV. 35 U.S.C. § 103, Obviousness

Claims 1, 15, 29, and 39 stand rejected under 35 U.S.C. § 103 as being unpatentable over Thompson et al. (U.S. Patent No. 5,430,842), hereinafter "Thompson" in view of Hefferon et al. (5,659,756), hereinafter "Hefferon" and Bean et al. (U.S. Patent No. 4,843,541), hereinafter "Bean". This rejection is respectfully traversed.

With respect to Claim 1, such claim recites "*responsive to receiving* the data packet at a first partition in the interpartition virtual network from a second partition in the interpartition virtual network in the logical partitioned data processing system, *identifying a state of a first flag and a state of a second flag in the data packet*" (emphasis added by Applicants). As can be seen, these features with respect to Claim 1 are associated with an action that occurs when a data packet is *received*, including the identification of the state of two flags that are in this received data packet. In rejecting this aspect of Claim 1, the Examiner states that Thompson teaches such data packet reception processing, citing Thompson col. 3, lines 40-49 and col. 8, lines 13-27. Applicants show that there, Thompson states:

> "In the inbound direction, network adapter 12 decodes the packet header and programs the checksum control information directly into internal registers. The network adapter 12 calculates the checksum as it transfers the packet to memory 11. When the network adapter 12 completes the calculation of the checksum, network adapter 12 appends the result to the data stream that is being transferred to the memory 11. The processor 15 compares this checksum result against the packet checksum to verify the data" (Thompson col. 3, lines 40-49) (emphasis added by Applicants); and
>
> "For example, FIG. 8 shows an *outbound packet 60 built in memory 11* (shown in FIG. 1). Outbound packet 60 includes a checksum control header 61, a link level header 62, an

> IP header 63, a transport header 64 and user data 65. Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76. Start offset field 71 indicates the byte at which checksumming is to start. Stop offset field 75 indicates the stop offset, that is, the number of bytes which are to be checksummed. Algo field 72 indicates the checksum algorithm used (TCP, UDP, etc.). Direction field 73 indicates the direction of data flow (inbound or outbound). Insert field 74 indicates whether the *outbound* packet is to have a checksum *inserted*. Insert offset field 76 indicates the location where a checksum is to be inserted" (Thompson col. 8, lines 13-27) (emphasis added by Applicants).

As to the cited passage at Thompson col. 3, such passage describes various operational steps that are performed when a data packet is *received*. The cited passage at Thompson col. 8, however, describes various operational steps that are performed when a data packet is to be *transmitted*. The receipt and transmission of data packets are separate and distinct operations, and steps describing operational steps with respect to *transmission* of data packets, such as those described by Thompson at col. 8, do not provide any description or teaching with respect to operational steps that occur upon *receiving* a data packet, which is what Claim 1 is directed to. Thus, Thompson's description at col. 8 does not provide any teaching as to any operational steps that occur "responsive to receiving" a data packet, as is recited in Claim 1. Thus, the Examiner's reliance on Thompson's teachings at col. 8 – which is directed to steps that occur in anticipation of a data packet being *transmitted* - does not provide any teaching/description of any operational steps that occur *responsive to receiving* the data packet, as per the features of Claim 1.

As to the cited Thompson passage at col. 3, which is directed to steps that occur when receiving a data packet, this description describes a traditional checksum calculation being unconditionally performed by the network adapter, including steps of decoding, programming, calculating, transferring, appending and comparing. Such traditional checksum calculation has already been expressly acknowledged by Applicants in the background section of their own Specification (page 1, lines 12-27; "Description of Related Art"). This unconditional checksum processing of received packets by a network adapter has been improved upon by the present invention, where the checksum is advantageously *selectively verified* – and such selective verification of the checksum occurs as indicated by the state of the first flag and the second flag. Thompson's teachings at col. 3 with respect to checksum processing *occurs unconditionally*, and such checksum processing is not described as being performed 'as indicated by the state of the first flag and the state of the second flag', as per the features of Claim 1. Instead, this cited passage states that the packet header is 'decoded', a checksum is 'calculated', which is then 'compared' with the received checksum in the received data packet. There is *no selective verification of the checksum of a received data packet as indicated by the state of* ***two flags that are received***, as per the features expressly recited in Claim 1.

Further with respect to Thompson's description at col. 8 regarding outbound packet data processing, to the extent such passage describes flags, these flags do not indicate whether to selectively verify a checksum in a received data packet, but instead *indicate whether a checksum is to be inserted in an outbound packet*. This is different from Claim 1 in that 'insertion' of a checksum is substantially different from 'verifying' a checksum, and processing associated with an 'outbound' packet has nothing to do with processing of an inbound/received data packet, as per the features of Claim 1. Nor are these flags described as being part of a data packet that is received, as per the features of Claim 1. Thus, it is further shown that Claim 1 has been erroneously rejected as Thompson's flags are not used to indicate selective *verification* of a *received* data packet, but instead indicates whether a checksum is to be *inserted* in an *outbound* data packet.

Nor do the other cited references to Hefferon and Bean overcome such teaching deficiency. For example, Hefferon does not describe any type of checksum processing. As further example, Bean does not describe any type of checksum processing. Thus, it is urged that Claim 1 has been erroneously rejected as the Examiner has failed to properly establish a prima facie showing of obviousness. [1]

Applicants traverse the rejection of Claims 15 and 29 for similar reasons to those given above with respect to Claim 1.

With respect to Claim 39, such claim has previously been cancelled (responsive to a Restriction Requirement dated September 17, 2007), and so it is unclear why Claim 39 is being rejected in the current Office Action dated July 3, 2008. Further clarification is requested regarding the rejection of Claim 39.

Therefore, the rejection of Claims 1, 15, 29, and 39 under 35 U.S.C. § 103 has been overcome.

## V. 35 U.S.C. § 103, Obviousness

Claims 1-39 stand rejected under 35 U.S.C. § 103 as being unpatentable over Maezawa et al. (U.S. Patent No. 6,145,024), hereinafter "Maezawa" in view of Kondo et al. (U.S. Patent No. 6,618,396), hereinafter "Kondo" and Lansing et al. (U.S. Publication No. 2003/0058862), hereinafter "Lansing" in further view of Thompson in view of Herron and Bean. This rejection is respectfully traversed.

---

[1] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id.* All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP 2143.03; *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In the absence of a proper *prima facie* case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent. *See In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

Generally speaking with respect to Claim 1, it is urged that the combined teachings of the cited references describe a conditional CRC *check* based on a single ECC flag (Kondo), and a conditional CRC *generation* (but not a check) based on a single CRC flag (Lansing). Thus, the combination does not teach a conditional CRC *check* based on *two* different flags (a first flag *and* a second flag). It is further urged that none of the cited references teach or otherwise suggest sending data packets from one logical partition of a logical partitioned data processing system to another partition within the same logical partitioned data processing system using virtual network adapters, as per the interpartition virtual network features provided by amended independent Claims 1, 15, 29 and 39.

With respect to Claim 1, such claim recites "selectively verifying a checksum, by the first partition in the logical partitioned data processing system, for the data packet as indicated by the state of the first flag and the state of the second flag, wherein the first flag and the second flag are both checksum-based flags that indicate checksum characteristics associated with the data packet". As can be seen, such claimed features are directed to a conditional CRC *check* based on *two* different flags. In reaching the conclusion that all three references (Kondo, Maezawa and implicitly in Lansing) describe a CRC check being based on a CRC flag (which Applicants deny, as will be further shown below), the Examiner mischaracterizes the teachings of the cited reference. For example, on page 10 of the present Office Action dated July 3, 2008, the Examiner states:

> "the flag in Kondo providing an indication of whether redundancy exists"

Applicants urge clear error in such assertion, as the Kondo flag does not provide any indication of *whether redundancy exists* – instead the Kondo flag provides an indication of *whether an ECC error exists*. An ECC error indicator does not provide any information as to whether *redundancy* exists, but instead provides an indication of whether an *error* exists. This can be seen by Kondo's description at col. 39, lines 62-65, where it states:

> "When checking the CIP header 2701, the ECC flag 2702 contained therein is examined. When the **ECC flag indicates "no ECC error"**, CRC check on the AV data 2704 is performed."

Thus, contrary to the Examiner's assertion, Kondo's flag does not provide any indication of whether redundancy exists, but instead provides an indication of whether an error exists. As this Kondo mischaracterization is used in establishing why the claims are obvious in view of the cited references, it is urged that such obviousness conclusion is flawed as relying upon such improper characterization of what Kondo actually describes.

Still further, the Lansing flag is not used in determining whether to *verify* as a checksum. Instead, the Lansing flag is used to determine whether to *generate* a checksum (Lansing Figure 9, element 905, the "Generate CRC Flag"). Thus, even when the teachings of Kondo and Lansing are combined, such combination does not describe the *use of two flags in a selective verify step*, as per the features of Claim 1. Instead, such resulting combination describes one flag being used to indicate whether an error exists, and if so a CRC is verified, and the other flag is used to determine whether to 'generate' a CRC (in contradistinction to 'verifying' a CRC, as per Claim 1).

Further with respect to Claim 1, the cited Maezawa reference describes, as expressly acknowledged by the Examiner, that *each packet has a CRC checksum* used for verifying received data (see page 9 of the present Office Action dated July 3, 2008, lines 6-9), and thus it is urged that a person of ordinary skill in the art would not have been motivated to modify such Maezawa teachings of verifying *each* packet in accordance with the claimed feature of '*selectively* verifying' due to this Maezawa desire to verify each packet. Thus, the only motivation for making such a change must be coming from Applicants' own disclosure and claims, which is impermissible hindsight analysis.[2]

Claim 1 also recites interpartition packet features. Specifically, Claim 1 recites "responsive to receiving the data packet at a first partition in the interpartition virtual network from a second partition in the interpartition virtual network in the logical partitioned data processing system, identifying a state of a first flag and a state of a second flag in the data packet". As can be seen, the flag states are identified 'responsive to receiving the data packet at a first partition in the interpartition virtual network from a second partition in the interpartition virtual network in the logical partitioned data processing system'. None of the cited references teach receiving such an interpartition data packet, and thus none of the cited references teach an action being performed (e.g., 'identifying') that occurs 'responsive to receiving' such (missing) interpartition data packet. In rejecting this aspect of Claim 1, the Examiner states that Maezawa teaches receiving such an interpartition data packet. For example, on page 8 of the present Office Action, at the bottom of the page, the Examiner states:

> "Maezawa teaches receiving a data packet at a first partition in the interpartition virtual network from a second partition in the interpartition virtual network in the logical partitioned data processing system (col. 3, lines 60-65, col. 12, lines 1-12 and Figure 1)"

[2] It is error to reconstruct the patentee's claimed invention from the prior art by using the patentee's claims as a "blueprint". When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985).

Applicants urge that the Maezawa description does not describe the claimed 'interpartition virtual network' since such reference does not describe "wherein each one of the logical partitions comprises a virtual network **adapter** that is used to send data packets to other virtual network **adapters** of other logical partitions within the logical partitioned data processing system *to thereby form the interpartition virtual network*". As Claim 1 explicitly defines the claimed 'interpartition virtual network' to be a network where each one of the logical partitions comprises *a virtual network adapter that is used to send data packets to other virtual network adapters* of other logical partitions within the logical partitioned data processing system, and the cited Maezawa reference does not describe such virtual network adapters or their associated claimed features, Maezawa cannot describe or teach the claimed interpartition virtual network. Accordingly, as Maezawa cannot describe/teach the claimed interpartition virtual network, it necessarily logically follows that Maezawa also cannot describe/teach data packet transfer in such a (missing) interpartition virtual network. Thus, contrary to the Examiner's assertion in rejecting Claim 1, Maezawa does not teach the claimed interpartition virtual network, or the receiving of a data packet at a first partition of such (missing) interpartition virtual network. Thus, it is further urged that Claim 1 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further yet with respect to Claim 1, the Examiner has mischaracterized the teachings of the cited Thompson reference in their attempt to establish prima facie obviousness. The Examiner cites Thompson's col. 3, lines 40-49 and col. 8, lines 13-27 as teaching the claimed feature of responsive to receiving a data packet at a first partition from a second partition, identifying a state of two flags. Applicants urge clear error in such assertion, as will now be shown in detail.

As to the cited Thompson passage at col. 3, which is directed to steps that occur when receiving a data packet, this description describes a traditional checksum calculation being unconditionally performed by the network adapter, including steps of decoding, programming, calculating, transferring, appending and comparing. Such traditional checksum calculation has already been expressly acknowledged by Applicants in the background section of their own Specification (page 1, lines 12-27; "Description of Related Art"). As to the cited Thompson passage at Col. 3, which is directed to steps that occur when receiving a data packet, this description describes a traditional checksum calculation being unconditionally performed by the network adapter, including steps of decoding, programming, calculating, transferring, appending and comparing. Such traditional checksum calculation has already been expressly acknowledged by Applicants in the background section of their own Specification (page 1, lines 12-27; "Description of Related Art"). The operational steps with respect to *transmission* of data packets, such as those described by Thompson at the cited col. 8 passage, do not provide any description or teaching with respect to operational steps that occur upon *receiving* a data packet, which is what Claim 1 is directed to. Quite simply, Thompson's description at col. 8 does not provide any teaching as to any

operational steps that occur "responsive to receiving" a data packet, as is recited in Claim 1. Thus, the Examiner's reliance on Thompson's teachings at col. 8 – which is directed to steps that occur in anticipation of a data packet being *transmitted* - does not provide any teaching/description of any operational steps that occur *responsive to receiving* the data packet, as per the features of Claim 1. Thus, the Examiner's characterization of the Thompson teachings is clearly erroneous – further evidencing that Claim 1 has been erroneously rejected.

Applicants initially traverse the rejection of Claims 2-14 for reasons given above with respect to Claim 1 (of which Claims 2-14 depend upon).

Further with respect to Claim 2 (and dependent Claims 3-10), it is urged that none of the cited references teach or suggest the claimed feature of "wherein the first flag is a no checksum flag that is used by the selectively verifying step to determine whether or not there is a checksum value included in the data packet that is received and *the second flag is a checksum good flag that is used by the selectively verifying step to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received*". As can be seen, the features of Claim 2 are directed to features/characteristics associated with the two flags. Specifically, the first flag is a no checksum flag that is used by the selectively verifying step to determine whether or not there is a checksum value included in the data packet that is received. The second flag is a checksum good flag that is used by the selectively verifying step to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received. In rejecting Claim 2, the Examiner cites Kondo col. 39, lines 55-67 and Lansing's step 905 of Figure 9 as teachings the features of Claim 2. Applicants urge clear error in such assertion, as will now be described in detail.

Kondo describes at col. 39, line 55-67 an ECC flag that indicates whether or not there is an ECC error. Such ECC flag (1) is not used by a selectively verifying step to *determine whether or not there is a checksum value included in the data packet that is received* (and thus this ECC flag is not equivalent to the claimed first flag) – instead this flag indicates if there is an *error*, and (2) is not used by a selectively verifying step to determine whether or not the data packet *has previously been verified as being good* based on a checksum included in the data packet that is received (and thus this ECC flag is not equivalent to the claimed second flag) - instead this ECC flag indicates if there is an *error*.

Lansing describes at Figure 9, element 905 a CRC generation flag that indicates *whether or not a CRC is to be generated during packet transmission*. Such CRC generation flag (1) is not used by a selectively verifying step to *determine whether or not there is a checksum value included in the data packet that is received* (and thus this CRC generation flag is not equivalent to the claimed first flag) – instead this flag indicates if a *CRC should be generated* for a packet to be *transmitted*, and (2) is not used by a selectively verifying step to determine whether or not the data packet *has previously been verified as*

*being good* based on a checksum included in the data packet that is received (and thus this CRC generation flag is not equivalent to the claimed second flag) - instead this CRC generation flag indicates if *CRC should be generated* for a packet to be *transmitted.*

Thus, neither of these cited passages describes *either one* of the two flags expressly recited in Claim 2, and therefore it is further urged that Claim 2 (and dependent Claims 3-10) has been erroneously rejected due to this additional prima facie obviousness deficiency.

The Examiner further states that Claim 2 recites data attributes of two data elements, but fails to recite a concrete limitation that concretely provides an additional limitation further limiting Claim 1. Applicants urge clear error in such assertion, as Claim 1 recites a step of 'selectively verifying' and Claim 2 recites (1) "wherein the first flag is a no checksum *flag that is* ***used by the selectively verifying step*** *to determine whether or not there is a checksum value included in the data packet that is received* and (2) the second flag is a checksum good *flag that is* ***used by the selectively verifying step*** *to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received*". Thus, contrary to the Examiner's assertions regarding Claim 2, the limitations of Claim 2 do in fact further limit the selectively verifying step recited in Claim 1.

Further with respect to Claim 4, such claim recites "wherein the selectively verifying step includes: skipping verification of the checksum if the first flag is set". As can be seen, the features of Claim 4 are directed to particulars associated with the *selectively verifying step*, where checksum verification is skipped if the first flag is set. The Examiner asserts that Lansing teaches such selectively verifying details at Figure 9, elements 905-915. Applicants urge clear error, as this cited Lansing passage: (1) is not directed to any type of *verification* step, but instead is directed to a *generation* step (Lansing Figure 9, element 910), and (2) does not describe any skipping of checksum *verification*, but instead is directed to skipping a checksum *generation* step (Lansing Figure 9, element 910). Thus, contrary to the Examiner's assertion, Lansing does not teach the features expressly recited in Claim 4, and therefore it is further urged that Claim 4 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 6, such claim recites "wherein the second flag is conditionally unset by the logical partitioned data processing system if the packet was received through a first virtual adapter associated with the first partition". As can be seen, the features of Claim 6 are specifically directed to a conditional unsetting of the second flag, where such condition is "if the packet was received through a first virtual adapter associated with the first partition". The Examiner makes no assertion as to any teaching with respect to the condition regarding how that packet was received, instead asserting that Claim 6 fails to recite a concrete limitation that further limits Claim 1. Applicants urge clear error in such assertion, as Claim 6 depends upon Claim 2 and defines a specific condition for which the second flag is

unset, and this second flag is *used* (per Claim 2) *by the selectively verifying step* (of Claim 1) to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received. Thus, Claim 6 in combination with Claim 2 (of which Claim 6 depends upon) does in fact further limit the features of Claim 1 (as Claim 2 depends upon Claim 1). Therefore, it is further urged that Claim 6 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 7, such claim recites "wherein the first flag is conditionally set by the logical partitioned data processing system if the data packet, received from the second partition, originated from within the logical partitioned data processing system". As can be seen, the features of Claim 7 are specifically directed to a conditional setting of the first flag, where such condition is "if the data packet, received from the second partition, originated from within the logical partitioned data processing system". The Examiner makes no assertion as to any teaching with respect to the condition regarding where the data packet originated, instead asserting that Claim 7 fails to recite a concrete limitation that further limits Claim 1. Applicants urge clear error in such assertion, as Claim 7 depends upon Claim 2 and defines a specific condition for which the first flag is set, and this *first flag is used* (per Claim 2) *by the selectively verifying step* (of Claim 1) to determine whether or not there is a checksum value included in the data packet that is received. Thus, Claim 7 in combination with Claim 2 (of which Claim 7 depends upon) does in fact further limit the features of Claim 1 (as Claim 2 depends upon Claim 1). Therefore, it is further urged that Claim 7 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 8 (and dependent Claims 9 and 10), such claim recites "wherein the second flag is conditionally unset by the logical partitioned data processing system if the data packet, received from the second partition, was received from outside the interpartition virtual network in the logical partitioned data processing system without the checksum being checked". As can be seen, the features of Claim 8 are specifically directed to conditionally unsetting the second flag, where such condition is "if the data packet, received from the second partition, was received from outside the interpartition virtual network in the logical partitioned data processing system without the checksum being checked". The Examiner makes no assertion as to any teaching with respect to the condition regarding how that packet was received, instead asserting that Claim 8 fails to recite a concrete limitation that further limits Claim 1. Applicants urge clear error in such assertion, as Claim 8 depends upon Claim 2 and defines a specific condition for which the second flag is unset, and this second flag is *used* (per Claim 2) *by the selectively verifying step* (of Claim 1) to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received. Thus, Claim 8 in combination with Claim 2 (of which Claim 8 depends upon) does in fact further limit

the features of Claim 1 (as Claim 2 depends upon Claim 1). Therefore, it is further urged that Claim 8 (and dependent Claims 9 and 10) has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 9, such claim recites "wherein the first flag is conditionally unset by the logical partitioned data processing system and the second flag is conditionally unset by the logical partitioned data processing system if the data packet was received by a physical network adapter that (i) is associated with the second partition, and (ii) does not support checksum offload". As can be seen, the features of Claim 9 are specifically directed to a conditional unsetting of the first and second flags, where such condition is "if the data packet was received by a physical network adapter that (i) is associated with the second partition, and (ii) does not support checksum offload". The Examiner makes no assertion as to any teaching with respect to the condition regarding where the data packet originated, instead asserting that Claim 9 fails to recite a concrete limitation that further limits Claim 1. Applicants urge clear error in such assertion, as Claim 9 depends upon Claims 2 and 8 and defines a specific condition for which the first and second flags are unset, and these *first and second flags are used* (per Claim 2) *by the selectively verifying step* (of Claim 1) to determine (1) whether or not there is a checksum value included in the data packet that is received, and (2) to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received. Thus, Claim 9 in combination with Claims 2 and 8 (of which Claim 9 depends upon) does in fact further limit the features of Claim 1 (as Claim 2 depends upon Claim 1). Therefore, it is further urged that Claim 9 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 10, such claim recites "wherein the first flag is conditionally unset by the logical partitioned data processing system and the second flag is conditionally set by the logical partitioned data processing system if a physical adapter, supporting a checksum offload, verified the checksum as being good". As can be seen, the features of Claim 10 are specifically directed to a conditional unsetting of the first flag and conditional setting of the second flag, where such condition is "if a physical adapter, supporting a checksum offload, verified the checksum as being good". The Examiner makes no assertion as to any teaching with respect to the condition regarding where the data packet originated, instead asserting that Claim 10 fails to recite a concrete limitation that further limits Claim 1. Applicants urge clear error in such assertion, as Claim 10 depends upon Claims 2 and 8 and defines a specific condition for which the first flag is unset and the second flag is set, and these *first and second flags are used* (per Claim 2) *by the selectively verifying step* (of Claim 1) to determine (1) whether or not there is a checksum value included in the data packet that is received, and (2) to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received. Thus, Claim 10 in combination with Claims 2 and 8 (of which Claim 10

depends upon) does in fact further limit the features of Claim 1 (as Claim 2 depends upon Claim 1). Therefore, it is further urged that Claim 10 has been erroneously rejected due to this additional prima facie obviousness deficiency.

With respect to Claim 11, such claim recites "wherein the first virtual adapter is a software device driver that has no associated physical hardware". In rejecting Claim 11, the Examiner states that Maezawa teaches the features of Claim 11 by Maezawa's multiplexor channel devices 3 and 10 in Figure 1. Applicants urge that such physical hardware devices do not teach "wherein the first virtual adapter is a software device driver *that has no associated physical hardware*", as per the features of Claim 11. Therefore, it is further urged that Claim 11 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 12, such claim recites "conditionally generating the checksum for the new data packet only if the new data packet is to be sent outside of the interpartition virtual network by a physical network adapter". As can be seen, the checksum generation is conditional, with such condition being "*only if* the new data packet is to be sent *outside* of the interpartition virtual network by a physical network adapter". In rejecting this aspect of Claim 12, the Examiner cites Maezawa's circuit 37 in Figure 2 as teaching such claimed limitation. Applicants urge clear error, as this circuit 37 is not described as generating checksums, as per the features of Claim 12, but instead is used for transmitting frames (Maezawa col. 11, lines 27-32). Therefore, it is further urged that Claim 12 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Further with respect to Claim 13, such claim recites "wherein the first flag and the second flag are added to a header of the data packet that is received by firmware of the logical data processing system during routing of the data packet, to a given partition of the logical partitioned data processing system, by the firmware". As can be seen, the features of Claim 13 are specifically directed to a particular technique for adding flags to a header of a data packet. In rejecting Claim 13, the Examiner states that Maezawa teaches a means for sending by Maezawa's circuits 37 and 38 of Figure 2. Applicants urge clear error, as Claim 13 was previously amended to recited data packet header operations in combination with firmware, and does not recite any type of means for sending, as alleged by the Examiner. Therefore, it is further urged that Claim 13 has been erroneously rejected due to this additional prima facie obviousness deficiency.

Applicants initially traverse the rejection of Claims 15-38 for similar reasons to those given above with respect to Claim 1.

Applicants further traverse the rejection of Claims 16 (and dependent Claims 17-24) and 30 (and dependent Claims 31-38) for similar reasons to the further reasons given above with respect to Claim 2.

Applicants further traverse the rejection of Claims 18 and 32 for similar reasons to the further reasons given above with respect to Claim 4.

Applicants further traverse the rejection of Claims 20 and 34 for similar reasons to the further reasons given above with respect to Claim 6.

Applicants further traverse the rejection of Claims 21 and 35 for similar reasons to the further reasons given above with respect to Claim 7.

Applicants further traverse the rejection of Claims 22 and 36 for similar reasons to the further reasons given above with respect to Claim 8.

Applicants further traverse the rejection of Claims 23 and 37 for similar reasons to the further reasons given above with respect to Claim 9.

Applicants further traverse the rejection of Claims 24 and 38 for similar reasons to the further reasons given above with respect to Claim 10.

Applicants further traverse the rejection of Claim 25 for similar reasons to the further reasons given above with respect to Claim 11.

Applicants further traverse the rejection of Claim 26 for similar reasons to the further reasons given above with respect to Claim 12.

Applicants further traverse the rejection of Claim 27 for similar reasons to the further reasons given above with respect to Claim 13.

With respect to Claim 39, such claim has previously been cancelled (responsive to a Restriction Requirement dated September 17, 2007), and so it is unclear why Claim 39 is being rejected in the current Office Action dated July 3, 2008. Further clarification is requested regarding the rejection of Claim 39.

Therefore, the rejection of Claims 1-39 under 35 U.S.C. § 103 has been overcome.

## VI. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: August 14, 2008

Respectfully submitted,

/Wayne P. Bailey/

Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants